CLAIMS

What is claimed is:

1. A method comprising:

detecting a data signature; and

correlating said data signature with a fingerprint of the target to determine to what extent said target is vulnerable to said data signature.

2. The method as in claim 1 further comprising:

evaluating contextual information related to said data signature to determine a likelihood that said target is under attack.

3. The method as in claim 1 wherein said fingerprint includes said target node's operating system version.

4. The method as in claim 1 wherein said fingerprint includes said target node's processor type.

5. The method as in claim 2 wherein said contextual information includes a particular network protocol with which said data signature was transmitted.

6. The method as in claim 1 further comprising:

generating a first alert condition upon determining that said target node is vulnerable to said data signature.

7. The method as in claim 1 further comprising:

listening for a response to said data signature from said target.

8. The method as in claim 7 further comprising:

determining whether said target node's response or lack of a response is suspicious.

9. The method as in claim 8 wherein determining whether said target's response is suspicious comprises determining whether said target's response is an "unknown command" response.

10. The method as in claim 8 further comprising:

generating a second alert condition upon determining that said target node's response or lack of a response is suspicious

11. The method as in claim 10 further comprising:

combining the second alert with the first, thereby updating the first alert with information within the second alert.

12. The method as in claim 1 further comprising:

listening for behavior of said target node; and

generating a second alert condition upon determining that said target node's behavior is suspicious.

13. The method as in claim 11 wherein said target node's suspicious behavior comprises transmitting a root shell prompt to a suspect node.

14. A method comprising:

identifying a data signature directed at a target;

evaluating said data signature's context; and determining whether said data signature poses a threat based on said context of said data signature.

15. The method as in claim 14 wherein said data signature's context is a particular protocol used to transmit said data signature.

16. The method as in claim 15 wherein said protocol is the HyperText Transport Protocol ("HTTP").

17. The method as in claim 16 further comprising:

determining that said data signature poses a threat if said data signature is "/cgi-bin/phf" embedded in the header of said HTTP data transmission.

18. The method as in claim 14 further comprising

evaluating whether said data signature poses a threat based on a fingerprint of said target.

19. The method as in claim 18 wherein said fingerprint is comprised of a particular service executed on said target.

20. The method as in claim 18 wherein said fingerprint is comprised of a particular operating system executed on said target.

21. The method as in claim 18 wherein said fingerprint is comprised of a particular hardware platform of said target.

22. The method as in claim 14 further comprising:

monitoring responses from said target following said data signature; and

determining a likelihood of whether said target is under attack based on data signatures of said responses.

23. The method as in claim 22 wherein said target response is a non-protocol response.

24. The method as in claim 23 wherein said data signature is transmitted to the target using the file transfer protocol ("FTP") and said non-protocol response indicates a raw shell connection to said target.

25. A method comprising:

monitoring a plurality of data transmissions between a suspect and a target, said data transmissions indicating a current state of communication between said suspect and said target; and

evaluating a likelihood that said target is under attack based on one or more data signatures of said transmissions and said current state of communication.

26. The method as in claim 25 wherein said current state of communication is based on a known protocol with which said data transmissions are transmitted/received between said suspect and target.

27. The method as in claim 26 wherein said known protocol is FTP.

28. The method as in claim 27 wherein one of said data signatures is the filename "passwd" in a context in which filenames are likely to appear.

29. The method as in claim 25 further comprising:

monitoring responses from said target following said data signature; and

determining a likelihood of whether said target is under attack based on data signatures of said responses.

30. The method as in claim 25 wherein said current state comprises any outbound connection from said target is following a detected signature.

31. The method as in claim 25 wherein said current state comprises an inbound connection to a new port following a detected signature.

32. A method as in claim 25 monitoring said current state comprises:

profiling said target to determine which ports are open by passively listening to what traffic succeeds in talking to/from the target.

33. A method as in claim 25 monitoring said current state comprises:

detecting non-protocol requests or responses transmitted to/from said target.

34. The method as in claim 25 further comprising:

determining a fingerprint of said target; and

further evaluating a likelihood that said target is under attack based on said fingerprint.

35. The method as in claim 26 wherein said known protocol is HTTP

36. The method as in claim 26 wherein said known protocol is RPC.

37. A machine-readable medium having program code stored thereon which, when executed by a machine, causes said machine to perform the operations of:

detecting a data signature; and

correlating said data signature with a fingerprint of the target to determine to what extent said target is vulnerable to said data signature.

38. The machine-readable medium as in claim 37 further comprising program code to cause said machine to perform the operations of:

evaluating contextual information related to said data signature to determine a likelihood that said target is under attack.

39. The machine-readable medium as in claim 37 wherein said fingerprint includes said target node's operating system version.

40. The machine-readable medium as in claim 37 wherein said fingerprint includes said target node's processor type.

41. The machine-readable medium as in claim 38 wherein said contextual information includes a particular network protocol with which said data signature was transmitted.

42. The machine-readable medium as in claim 37 further comprising program code to cause said machine to perform the operations of:

generating a first alert condition upon determining that said target node is vulnerable to said data signature.

43. The machine-readable medium as in claim 37 further comprising program code to cause said machine to perform the operations of:

listening for a response to said data signature from said target.

44. The machine-readable medium as in claim 43 further comprising program code to cause said machine to perform the operations of:

determining whether said target node's response or lack of a response is suspicious.

45. The machine-readable medium as in claim 44 wherein determining whether said target's response is suspicious comprises determining whether said target's response is an "unknown command" response.

46. The machine-readable medium as in claim 44 further comprising program code to cause said machine to perform the operations of:

generating a second alert condition upon determining that said target node's response or lack of a response is suspicious

47. The machine-readable medium as in claim 46 further comprising program code to cause said machine to perform the operations of:

combining the second alert with the first, thereby updating the first alert with information within the second alert.

48. The machine-readable medium as in claim 37 further comprising program code to cause said machine to perform the operations of:

listening for behavior of said target node; and

generating a second alert condition upon determining that said target node's behavior is suspicious.

49. The machine-readable medium as in claim 47 wherein said target node's suspicious behavior comprises transmitting a root shell prompt to a suspect node.

50. A machine-readable medium having program code stored thereon which, when executed by a machine, causes said machine to perform the operations of:

identifying a data signature directed at a target;

evaluating said data signature's context; and

determining whether said data signature poses a threat based on said context of said data signature.

51. The machine-readable medium as in claim 50 wherein said data signature's context is a particular protocol used to transmit said data signature.

52. The machine-readable medium as in claim 51 wherein said protocol is the HyperText Transport Protocol ("HTTP").

53. The machine-readable medium as in claim 52 further comprising program code to cause said machine to perform the operations of:

determining that said data signature poses a threat if said data signature is "/cgi-bin/phf" embedded in the header of said HTTP data transmission.

54. The machine-readable medium as in claim 50 further comprising program code to cause said machine to perform the operations of:

further evaluating whether said data signature poses a threat based on a fingerprint of said target.

55. The machine-readable medium as in claim 54 wherein said fingerprint is comprised of a particular service executed on said target.

56. A machine-readable medium having program code stored thereon which, when executed by a machine, causes said machine to perform the operations of:

monitoring a plurality of data transmissions between a suspect and a target, said data transmissions indicating a current state of communication between said suspect and said target; and

evaluating a likelihood that said target is under attack based on one or more data signatures of said transmissions and said current state of communication.

57. The machine-readable medium as in claim 56 comprising program code to cause said machine to perform the additional operations of:

monitoring responses from said target following said data signature; and

determining a likelihood of whether said target is under attack based on data signatures of said responses.